

New-Scale SIEM

Cloud-native SIEM for fast, modern search, dashboarding, and coordinated response from a single workbench

Designed for Modern Security Operations

Logging data within an IT environment is a critical part of your enterprise security strategy. Every sensor, detection tool, and data feed drives more collection, often terabytes per day. With growing data volumes and limited time to detect, investigate, and respond to threats, you need a faster, more efficient way to manage log collection, correlation, investigation, and response.

New-Scale SIEM is a cloud-native solution that unifies cloud, on-premises, and third-party log data, normalizing it for more effective threat detection, investigation, and response (TDIR). You get real-time, scalable visibility across your security environment, helping your team stay ahead of threats.

New-Scale SIEM simplifies security log management while giving you the power to detect and respond quickly. It provides a centralized workbench for investigation and response, with prebuilt correlation rules, integrated threat intelligence for better event context, and intuitive dashboards for streamlined analysis. With the ability to process data at enterprise scale, your team gains the speed and visibility needed to tackle modern security challenges.

Threat Center

Threat Center is built into New-Scale SIEM, giving you a dedicated workbench for TDIR. It improves analyst productivity by automating evidence collection, tagging events, adding notes, and managing cases in a security-specific ticketing system.

Threat Center consolidates events and alerts from Exabeam and third-party security products so your team can review them individually or at scale. You can set automated triage conditions, escalate critical incidents, and collaborate across teams and time zones. By tracking incidents from discovery through resolution, you maintain complete visibility into your security operations and cut remediation times by up to 50%.

Exabeam Nova

Exabeam Nova, a team of AI agents embedded in New-Scale SIEM, accelerates investigation and response without requiring manual oversight.

- **Search Agent:** Run complex searches in natural without advanced query skills. Whether you're looking for indicators of compromise (IoCs) or building queries for investigation, the Search Agent translates your questions into Exabeam Query Language (EQL) mapped to the Common Information Model (CIM). This makes advanced searches fast, accessible, and precise.
- **Analyst Assistant Agent:** A context-aware chat companion that helps during investigations. It answers case-specific questions instantly, provides relevant log context, and reduces time spent digging through raw data.
- **Investigation Agent:** Automates case summaries, threat analyses, and next steps. Classifies threats, identifies key attack vectors, and highlights top detections so you can prioritize or dismiss incidents quickly.
- **Threat Scoring Agent:** Continuously analyzes behavior and applies risk scores to prioritize the most security-relevant events, cutting through noise so you can focus on high-risk threats.
- **Visualization Agent:** Turns natural language queries into charts and dashboards, making it easy to visualize trends in logs, detections, and system performance.
- **Advisor Agent:** Provides leaders with daily reports on SIEM coverage, MITRE ATT&CK® alignment, and use case adoption, helping demonstrate program value and identify where additional log data is needed.

Exabeam Nova automates evidence collection, correlates detections, and provides actionable insights to help you respond faster and more accurately.

Outcomes Navigator

Outcomes Navigator is integrated with New-Scale SIEM to map your data sources against security use cases and the ATT&CK framework. It highlights gaps in detection coverage, recommends additional log sources, and provides defensible metrics you can share with leadership. With peer benchmarking and boardroom-ready reports, you can demonstrate security program value and guide smarter investments.

Automation Management

Automation Management helps you standardize response workflows and automate repetitive tasks. With prebuilt playbooks and a no-code editor, you can coordinate response actions, escalate incidents, and send notifications within clicks of discovery. Hundreds of prebuilt integrations make it easy to extend automation across your security ecosystem.

Common Information Model (CIM)

Before you can analyze and correlate security data, it must be normalized. The Exabeam CIM standardizes how log data is parsed, stored, and viewed across vendors. This ensures compatibility with new log sources and use cases.

Built on the New-Scale Security Operations Platform

New-Scale SIEM is built on the cloud-native New-Scale Security Operations Platform, sold as New-Scale Fusion. New-Scale Fusion gives you a scalable foundation for collecting and analyzing log data, detecting attacks with behavioral analytics, and automating incident response. Dashboards provide a real-time view of uptime, system health, and data flows for all services, logs, and applications. The platform continuously strengthens your security posture by recommending ways to optimize event streams, refine parsing configurations, and close use case gaps.

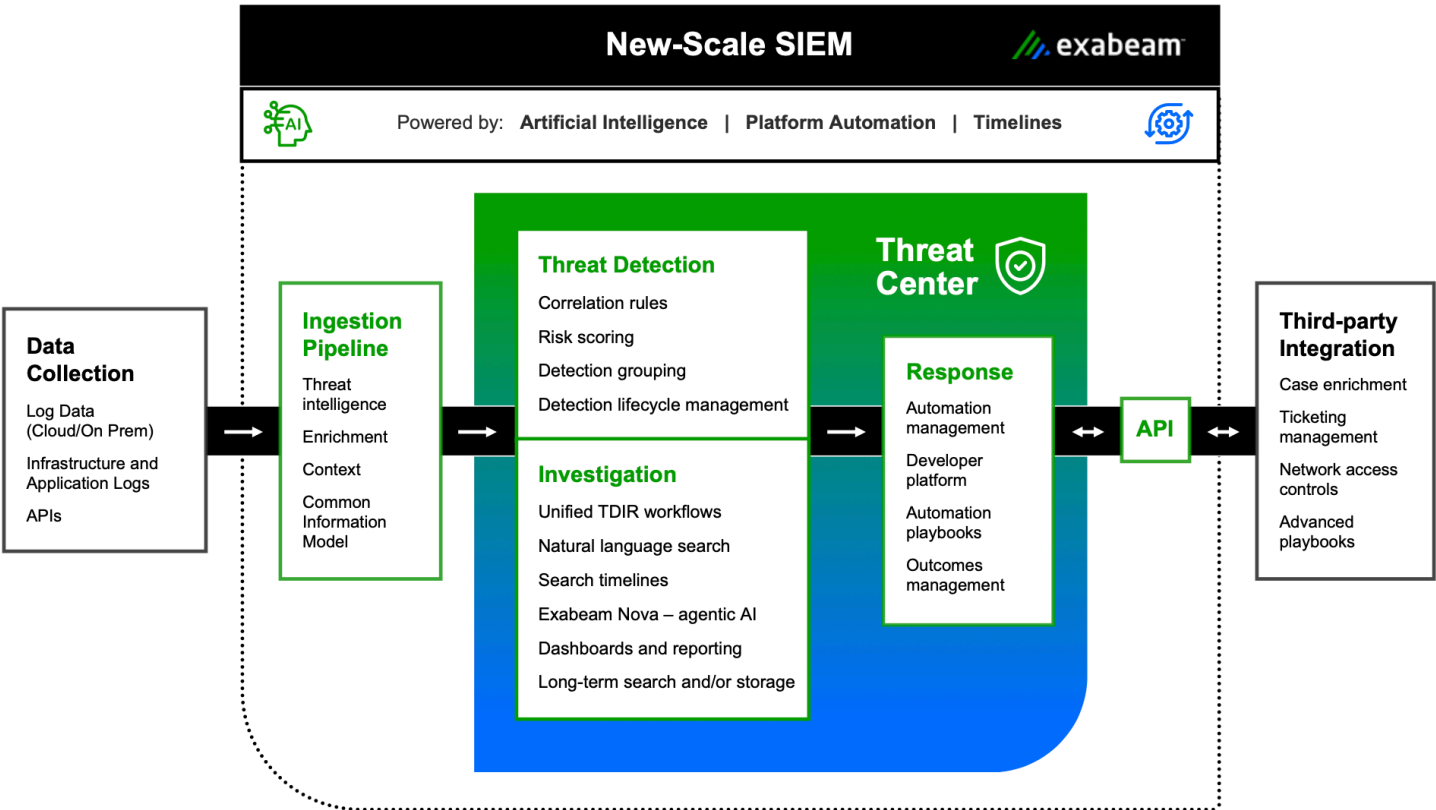


Figure 1. New-Scale SIEM unifies log collection, detection, investigation, and response in one cloud-native solution.

Benefits of New-Scale SIEM

- **Collect, store, and search with ease:** Centralize logs and context for TDIR with scalable storage and fast, intuitive search designed for all skill levels.
- **Turn raw logs into actionable intelligence:** Normalize, categorize, and transform log data with the CIM. Detect threats faster with structured data and easily create or modify parsers to support new sources.
- **Hunt threats proactively:** Search for IoCs and correlated events mapped to use cases and ATT&CK.
- **Automate response actions:** Use Automation Management to coordinate investigations, assign tasks, and send notifications as soon as threats are detected.
- **Simplify SOC integrations:** New-Scale Fusion is the first SOC platform to support the OpenAPI Standard (OAS), making it easier to onboard data sources, build automations, and streamline workflows across third-party tools.
- **Report on compliance standards:** View and export events for PCI, HIPAA, and other frameworks with prebuilt dashboards.
- **Close security gaps:** Outcomes Navigator maps your data sources to security use cases and ATT&CK tactics, techniques, and procedures (TTPs), identifying coverage gaps and recommending improvements.
- **Monitor SOC health and usage:** Track uptime, parser performance, and license consumption to ensure availability and plan capacity.
- **Easily extend detection:** Add New-Scale Analytics to incorporate behavioral analytics and detect anomalies for both human and non-human entities. It adapts to your environment, baselines normal activity, and flags unusual behavior so your team can focus on the most important threats.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).



Learn more at www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

2025 Exabeam, LLC. All rights reserved.